REMARKS

Claims 1-52 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 103(a) Rejection:

The Office Action rejected claims 1-7, 9-13, 15-24, 26-31, 33-41, 43-49 and 51-52 under 35 U.S.C. § 103(a) as being unpatentable over Hu (U.S. Patent 5,586,260) in view of Shambroom (U.S. Patent 6,301,661). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 1, Applicants disagree with the Examiner's contention that Hu teaches a client-side authentication library deployed on one or more client computer system, wherein the client-side authentication library comprises a client-side interface which is operable to retrieve and encrypt a user profile associated with a user. Hu teaches a method and apparatus for authenticating a client for a server when the client and server have different security mechanisms. Specifically, in Hu an *intermediary system* known as an authentication gateway provides for authentication of the client using the client security mechanism, and impersonation of the client in a call to a server that the client wishes to access (Hu, Abstract).

Specifically, Hu fails to teach an authentication library on a client system that can retrieve and encrypt a user profile. Instead, Hu teaches a system wherein a client system relies upon an *authentication gateway system*, separate from both the client system and server system, that authenticates the client system and stores client credentials on the authentication gateway system (Hu, Abstract, column 2, lines 1-19, lines 26-41). Hu clearly describes the authentication gateway system as being separate and distinct from the client system. Additionally, when describing Figure 1, Hu refers to three computer systems: a client system 10, a server system 12, and an authentication gateway computer system 14 (Hu, Figure 1, and column 3, lines 58-65). According to Hu, the

authentication gateway system obtains "in the authentication gateway system, a set of security credentials that will permit client access to the server" (Hu, column 2, lines 5-7). Under Hu's system the only thing retrieved on the client system is an access key or server-domain identity that "has no significance other than as a means for the authentication gateway to match a user with the credentials acquired during a log-in procedure" and it "does not need to be meaningful within the server security domain, and may even be numeric" (Hu, column 5, lines 33-48). Thus, rather than teaching a client-side interface operable to retrieve and encrypt a user profile, Hu teaches an authentication gateway system, separate from any client system that may save authentication credentials and also teaches that the client system only receives and saves an identifier associated with those credentials. While some client interface in Hu may have some interface by which it communicates with the authentication gateway system, there is no teaching in Hu that any interface on the client encrypts anything. Furthermore, there is no teaching in Hu that any interface on the client is implemented in accordance with a platform-independent interface specification.

Moreover, Hu fails to teach a server-side authentication library that comprises a server-side interface operable to receive the encrypted user profile from the client-side authentication library and decrypt the user profile to authenticate the user, as the Examiner contends. In contrast, Hu teaches an authentication gateway system, which is separate and distinct from the client system, that uses client credentials saved previously on the authentication gateway system, to "impersonate the client and call the server on the client's behalf" (Hu, column 2, lines 13-17). Since, according to Hu, a proxy server executing on an authentication gateway system impersonates the client and authenticates with the server, any information the server uses to authentication the client is not received from a client-side authentication library, but rather is received from the proxy server residing on the authentication gateway system. Also, since the gateway in Hu appears to the server as a client, it clearly cannot be considered a server-side authentication library. Nowhere does Hu teach a server-side interface which is operable to receive the encrypted user profile from the client-side authentication library, as the Examiner asserts. In fact, Hu very clearly teaches away from this by using a separate authentication gateway

system, thereby ensuring that authentication credentials, which the Examiner equates to a user profile are saved to the authentication gateway system and not the client system. Thus, it would be impossible for a server in Hu's system to receive an encrypted user profile from the client-side authentication library and decrypt the user profile to authenticate the user, as the Examiner holds.

In response to Applicants' previous arguments regarding a lack of motivation to modify Hu's system to use a platform-independent interface specification, the Examiner, in the Response to Arguments section, states that "the authentication gateway taught by Hu address the security mechanism in the lower layer of the network while the platform independent interface feature serves the purpose at the upper layer of the network" (Final Office Action, page 2, lines 17-19). However, Hu does not discuss anything in regard to upper and lower network layers. Furthermore, Applicants note that the Examiner's proposed modification of Hu to include a platform independent interface feature serving the purpose of some "upper layer" of the network and specifically still using Hu's authentication gateway to address the security mechanism in some "lower layer" still fails to result in a system that includes a client-side interface implemented in accordance with a platform-independent interface specification, deployed on a client computer system, operable to retrieve and encrypt a user profile. In contrast, the Examiner's proposed modifications of Hu would result in a system that still uses Hu's authentication gateway system to obtain and store client credentials and a proxy system executing on the authentication gateway system to authenticate with a servers system on behalf of the client by impersonating the client. Furthermore, and for the same reason, such a modification of Hu would fail to result in a system wherein a server-side interface would receive an encrypted user profile from a client-side authentication library and decrypt the user profile to authenticate the user, as the Examiner contends. Thus, Applicants assert that not only is there no motivation or suggestion in Hu regarding the benefits of using a platform-independent interface specification in an "upper layer" of a network, such a modification would still not result in the features which the Examiner is relying upon for his rejection of applicants' claim 1.

The examiner admits that Hu does not disclose authentication modules implemented in accordance with a platform-independent specification, but argues that Shambroom discloses authentication modules implemented in accordance with a platform-independent interface specification. However, nowhere does Shambroom describe any authentication modules as being implemented in accordance with a platform-independent interface specification. The Examiner's cited passages (Shambroom, Abstract and column 2, lines 26-65) only refer to a client exchanging enciphered communication for authentication and remote login purposes. The Examiner's cited portion of Shambroom does not mention anything regarding authentication modules implemented in accordance with a platform-independent interface specification.

Furthermore, Applicants' disagree with the Examiner's contention that a modification of Hu to include the use of JAVA, presumably as disclosed by Shambroom, would result in a platform-independent interface. JAVA is a platform independent language, not a platform independent interface as the Examiner holds. While JAVA may be platform-independent programming language, it does not automatically or inherently create platform-independent *interfaces*. Programs developed in the JAVA language are not inherently implemented in accordance with a platform-independent interface specification. Interfaces used in JAVA programs are quite frequently specific to a particular application, for example. Thus, modifying Hu by using the JAVA language as supposedly taught by Shambroom does not result in a client-side library that is implemented in accordance with a platform-independent interface specification. Nor would such a combination result in a server-side library that is implemented in accordance with a platform-independent interface specification.

Therefore, the rejection of claim 1 is unsupported by the teachings of the cited art and withdrawal thereof is respectfully requested. Similar arguments apply in regard to independent claims 18 and 35.

Regarding claim 2, Hu fails to teach wherein the client-side authentication library is shared by a plurality of management applications. The Examiner cites column 5, lines 4-19 of Hu, however, his passage of Hu describes only how a client system connects to an authentication gateway system for authentications. Nowhere do Hu and Shambroom, either singly or in combination, teach a client-side authentication library that is shared by a plurality of management applications. Thus, the rejection of claim 2 is unsupported by the teachings of the cited art and withdrawal thereof is respectfully requested. Similar arguments apply in regard to claims 19 and 36.

Regarding claim 3, applicants' assert that Hu fails to disclose a network management system wherein the server-side authentication library is shared by a plurality of gateway components. The Examiner again cites Hu, column 5, lines 4-19 for support. Applicants point out however that this passage of Hu fails to make any mention whatsoever of a server-side authentication library. In fact, the cited passage describes how a client system communicates with an authentication gateway system, which Hu clearly describes as being separate and distinct from the server system (see, Hu Figure 1, and column 3, lines 58-65). Furthermore, neither Hu, nor Shambroom, either singly or in combination, teaches a server-side authentication library which is shared by a plurality of gateway components. The rejection of claim 3 is clearly unsupported by the cited art and it withdrawal is respectfully requested. Similar arguments apply in regard to claims 20 and 37.

Regarding claim 10, Hu does not teach a gateway which is coupled to one or more managers, wherein the gateway is configured to provide network management services to the one or more managers, and one or more pluggable authentication modules which are operable to provide authentication of a manager. The Examiner refers to col. 2, lines 1-19 and col. 4, line 59 – col. 5, line 19 of Hu. However, these portions of Hu only refer to Hu's authentication gateway, which the Examiner equates to the one or more pluggable authentication modules. However, there is no description in these or any other portions of Hu of a gateway which is *coupled to one or more managers*, wherein the gateway is configured to *provide network management* services to the one or more managers. Nor

does Shambroom disclose anything regarding a gateway coupled to one or more managers wherein the gateway is configured to provide network management services to the one or more managers.

Additionally, Hu fails to disclose one or more pluggable authentication modules operable to provide authentication of a manager based upon a user profile, as the Examiner contends. In the Response to Arguments, the Examiner interprets the single authentication library or gateway in Hu as "one or more pluggable authentication modules". However, Hu's authentication gateway is not a pluggable authentication library. In contrast, the gateway in Hu cannot be swapped out for another module and hence is not a *pluggable* module. There is clearly no description of Hu's authentication gateway as being pluggable. In fact, the presence of the same non-pluggable gateway is required by Hu's teachings because a client may only login to the authentication gateway once per day, but the gateway must be able to save and use the client's saved credentials at anytime after the client successfully logs in (see Hu, column 5, lines 7-12).

Furthermore, applicants disagree with the Examiner's interpretation of one or more pluggable modules which are operable to provide authentication of a manager based upon a user interface as merely an authentication library connected to one or more client computers (see, Response to Arguments, page 3, lines 5-8). The concept of managers is well understood in the art of network management and equating a manager to any client computer, as the Examiner has proposed, is clearly incorrect.

Additionally, the combination of Hu and Shambroom fails to teach "wherein the one or more pluggable authentication modules are accessible by the gateway and the one or more managers through a platform-independent interface, wherein the gateway is configurable to authenticate the user to receive the network management services using the pluggable authentication modules through the platform-independent interface." Shambroom teaches enhancing security for application using downloadable executable content wherein a client web browser uses a gateway to authenticate and communicate with a web server. Nowhere does Shambroom mention pluggable authentication

modules, nor does Shambroom ever describe that such modules are accessible by one or more managers. Since Hu also fails to disclose either pluggable authentication modules or managers, the combination of Hu and Shambroom clearly fails to disclose one or more pluggable authentication modules accessible by the gateway and the one or more managers through a platform-independent interface, as the Examiner contends.

Thus, the rejection of claim 10 is clearly not supported by the prior art and its removal is respectfully requested. Similar arguments apply in regard to claims 27 and 44.

Claims 8, 14, 25, 32, 42 and 50 are rejected as being unpatentable over Hu in view of Thompson (U.S. Patent 6,622,050). Applicants note that the Examiner has not shown that the portions of Thompson relied upon in the rejection are prior art to the present application. The present application was filed April 21, 2000, which is before the March 30, 2001 filing date of Thompson. Thompson claims the benefit of provisional application 60/193,881 filed March 31, 2000. The Examiner states, "the cited limitation is taught both in [the] Thompson patent and the provisional application." However, Applicants' respectfully remind the Examiner that to qualify as prior art based upon the provisional filing date, both the provisional application and the Thompson patent must disclose the relevant features relied upon in the rejection. Moreover, the Thompson patent is not entitled to the March 31, 2000 date as a section 102(e) prior art date unless at least one claim of the Thompson patent is supported (under 35 U.S.C. § 112) in the provisional application. Under 35 U.S.C. 119(e)(1), Thompson is not entitled to its provisional application's filing date as a prior art date unless at least one claim of the published utility application is supported (per 35 U.S.C. § 112) in the provisional application. The rejection is improper unless the Examiner can show that the Thompson patent has the necessary claim support in the provisional application to be entitled to the provisional application's filing date as its § 102(e) prior art date. See also M.P.E.P. § 2136.03(IV).

The Examiner has the burden of proof to produce the factual basis for the rejection. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S.

1057 (1968). Since the Examiner has not proven that both of the above requirements have been met for Thompson's teachings to qualify as prior art, the Examiner has not met this burden of proof and the rejection is improper. Specifically, the Examiner should point out the **exact portions** of the provisional application that support at least one claim of the Thompson patent and should **also** point out the **exact portions** of the provisional application relied upon for the rejection. See also 37 CFR 1.04(c)(2).

Furthermore, the Examiner states that a copy of the provisional application is being provided to show that both the Thompson patent and the provisional patent include the limitations relied upon in the rejection of claims 8, 14, 25, 32, 42 and 50. **However, no copy of the provisional application was received with the Office Action.** Applicants' request that the Examiner ensure that a copy of the relied upon provisional application be included in the next communication.

Applicants also assert that the rejections of numerous ones of the dependent claims are further unsupported by the cited art. However, since the rejections of each of the independent claims have been shown to be improper, a further discussion of the rejections of the dependent claims is not necessary at this time.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-48700/RCK.

Also enclosed herewith are the following items:

☒ Return Receipt Postcard

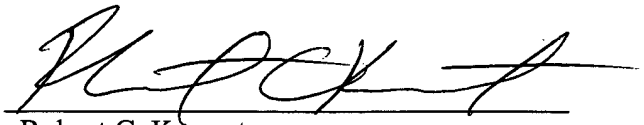
☐ Petition for Extension of Time

☐ Notice of Change of Address

☐ Fee Authorization Form authorizing a deposit account debit in the amount of $ for fees ( ).

☐ Other:

Respectfully submitted,



Robert C. Kowert
Reg. No. 39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: October 11, 2004